

Fraudele în mediul online sunt tot mai des întâlnite și este important să știi cum să le identifici și cum să te protejezi. De aceea dorim să te informăm cu privire la noile metode de fraudă utilizate de atacatori în ultima perioadă care vizează societăți comerciale din România, prin folosirea frauduloasă a identității Agenției Naționale de Administrare Fiscală (ANAF), a Casei Naționale de Asigurări de Sănătate (CNAS) și a instituțiilor bancare.

În ultima perioadă au fost semnalate mai multe tentative de fraudă de acest tip în mediul de afaceri, în care fraudatorii s-au prezentat drept reprezentanți ai ANAF, ai CNAS și ai unor bănci comerciale. Astfel, invocând proceduri de rambursare de TVA, ale contribuțiilor la sănătate sau datorii către ANAF, fraudatorii solicită acces la aplicațiile de Internet sau Mobile Banking prin intermediul aplicațiilor de control la distanță (de exemplu: AnyDesk, Rust Desk, TeamViewer).

Recomandări pentru evitarea fraudelor, protejarea fondurilor și a securității operațiunilor financiare:

- fiți vigilent cu privire la apelurile telefonice sau mesajele primite din partea persoanelor/numerelor necunoscute
- NU oferiți niciodată acces la aplicațiile de Internet sau Mobile Banking
- NU instalați aplicații la solicitarea unor persoane necunoscute
- NU furnizați date bancare, parole sau coduri de securitate
- NU accesați linkuri primite din surse suspecte
- verificați orice solicitare primită în numele unei instituții publice sau a unei bănci exclusiv prin canalele oficiale

Cum funcționează această fraudă?

- Fraudatorii exploatează încrederea mediului de afaceri în instituțiile publice și în sectorul bancar, utilizând tehnici de inginerie socială pentru a determina victimele să ofere acces la conturi sau la dispozitivele utilizate pentru operațiuni bancare.
- Fraudatorii contactează telefonic reprezentanții companiilor sau trimit link-uri false care par a veni de la instituțiile publice, pretinzând că reprezintă ANAF, CNAS, și invocă proceduri de rambursare de TVA sau a contribuțiilor la sănătate, respectiv datorii către ANAF.
- Sub pretextul acordării de sprijin, victimelor li se solicită să instaleze aplicații și să ofere acces la telefonul mobil și/sau la PC.
- În urma acestor acțiuni, fraudatorii urmăresc realizarea transferurilor neautorizate din conturile companiilor fraudate.

Atenție!!!

Băncile și instituțiile publice nu solicită acces la aplicațiile de Internet sau Mobile Banking, la ecranul dispozitivului sau instalarea aplicațiilor de control la distanță pentru realizarea de rambursări sau verificări ale conturilor.

În cazul în care suspectați o tentativă de fraudă sau ați fost deja victima unei astfel de fraude, este recomandată contactarea imediată a băncii și sesizarea autorităților competente.